International Journal of Electrical Engineering and Technology (IJEET)
Volume 11, Issue 8, October 2020, pp. 134-146, Article ID: IJEET_11_08_013
Available online at https://iaeme.com/Home/issue/IJEET?Volume=11&Issue=10
ISSN Print: 0976-6545 and ISSN Online: 0976-6553
https://doi.org/10.34218/IJEET.11.8.2020.013

TIED DOWN AODV ROUTING PROTOCOL TO IMPROVE SECURITY IN VANET

Dr. B. Senthilkumaran

Head and Assistant Professor, PG and Research Department of Computer Science, Jairams Arts and Science College, (affiliated to Bharathidasan University), Karur, Tiruchirappalli, Tamil Nadu, India

ABSTRACT

Vehicular specially appointed organizations (VANETs) are becoming promising and well known advances in the new insightful transportation world. They are utilized to give an Intelligent Transportation System(ITS), effective Traffic Information System (TIS), and Life Safety. This sort of organizations is entirely vulnerable to enemy's vindictive assaults, because of the unique changes of the organization geography, confiding in the hubs to one another, absence of fixed base for the investigation of hubs practices and compelled assets. One of these assaults is dark opening assault. In this assault, vindictive hubs infuse flaw steering data to the organization and lead all information parcels toward themselves, then, at that point obliterate them all. In this paper, we propose an answer, which upgrades the security of the Ad-hoc On-request Distance Vector (AODV) steering convention to experience the dark opening assaults. Our answer stays away from the dark opening and the different dark opening assaults. The reenactment results utilizing the Network Simulator NS2 shows that our convention gives better security and better execution as far as the bundle conveyance proportion than the AODV steering convention within the sight of one or various blackhole assaults with a minor ascent in normal start to finish delay and standardized directing overhead.

Keywords: Vehicular Ad Hoc networks, AODV routing protocol, security, Black hole attack

Cite this Article: B. Senthilkumaran, Tied down AODV Routing Protocol to Improve Security in VANET, *International Journal of Electrical Engineering and Technology (IJEET)*, 11(8), 2020, pp. 134-146.
https://iaeme.com/Home/issue/IJEET?Volume=11&Issue=10

1. INTRODUCTION

As of late, on account of a high number of street mishaps and with the improvement in the remote correspondence advances and Vehicular Ad hoc Network (VANET) are utilized to give a productive Traffic Information System (TIS). As indicated by the National Highway Traffic Safety Administration (NHTSA), vehicle-to-vehicle (V2V) correspondence has an extravagance and comfort saving potential that tends to around 80% of multi-vehicle crashes.

[1]. VANET is a subclass of Mobile Ad-hoc Network (MANET) which comprises of a few hubs (vehicles) communicating with one another without a fixed framework [2]. In any case, contrasted with MANET because of the great versatility of vehicles, VANET has an amazingly unique geography.

The hubs will in general move in a coordinated example [3]. Other than VANETs have a possibly largescale which can include numerous members and the ability to stretch out over the whole street network [4]. In this way, Lack of concentrated administration in VANET puts additional duties on vehicles. Subsequently every vehicle is a piece of the organization and furthermore oversees and controls the correspondence on that organization. The connections between vehicles interface are and separate all the time which makes directing interaction testing because of the great versatility of hubs. Thus, numerous analysts have zeroed in on steering in VANET. Which expects to mean to expand the Packet Delivery Ratio (PDR) and throughput while limiting bundle misfortune proportion and controlling overheads.

Toward this path many steering conventions have been proposed which has a significant job inorganizing the organization security. Be that as it may, impromptu steering conventions can be partitioned into receptive, proactive and cross breed conventions [5], responsive conventions don't occasionally refresh the directing data. It discovers the course just when required like Ad Hoc On-Demand Distance Vector (AODV) and Dynamic Source Routing (DSR). Proactive conventions are normally table-driven. Objective Sequence Distance Vector (DSDV), Global State Routing GCR are instances of this sort.

2. RELATED WORK

Dark Hole recognition has been a functioning space of examination and numerous arrangements have been proposed. In any case, a large portion of and requires high overhead to distinguish arrangements that have been proposed for MANETs that can be carried out in VANET. This segment examines a portion of these works. In [10], the creators proposed a way to deal with recognize dark opening hubs in the MANET. In the proposed technique, the identifying hub figures the proportion of the quantity of bundles dropped to an all out number of parcels sent effectively. This proportion is checked with a predefined edge worth to recognize any vindictive conduct. On the off chance that any mischief is discovered, the distinguishing hub attempts to stay away from the getting out of hand hub.

The creators in [11] proposed a plan (purported DCBA) to recognize and relieve dubious worth, which depends on the unusual distinction saw between the directing messages communicated from the hub. Besides, when the source hub gets the course answer (RREP) bundle in answer to the course demand (RREQ) parcel, they check the dubious worth of the hub that instated the RREP parcel. As check, assuming this worth is higher than the limit level, the hub is considered as noxious and its location is put away in a boycott table, forestalling that hub to additionally take an interest in the directing interaction. The proposed strategy in [12] projects a novel programmed security system utilizing Support Vector Machine (SVM) to shield against malevolent assault happening in AODV.

This strategy utilizes three measurements PDR (Packet Delivery Ratio), PMOR (Packet Modification Rate) and PMISR (Packet Misroute Rate), to choose the conduct of a hub. The data needed by the measurements is gathered from every one of the hubs in the organization. These measurements are contrasted with a limit, as per which the hub is considered malevolent or not. The creators in [13] propose a safeguard instrument against a helpful dark opening assault that depends on the AODV steering convention named SSP-AODV Protocol. They have consolidated two strategies: A* search calculation and Floyd- Warshall's calculation in the AODV steering measure. Furthermore, they have utilized the worth of bounce check and the assessed time as contribution to these two calculations to choose the most brief secure way. A

changed calculation to work on the security and execution of the AODV convention against the dark opening assault from in [14]. In this calculation, the creators utilized a few new principles to distinguish the ruinous hubs as per the hub's practices in an Ad Hoc arrange and erase them from directing.

Our proposed procedure varies from the strategies referred to on writing audit in that it centers around sending just the substantial course answer to the following hub, even on account of at least one blackhole assaults, by sending double a similar bundle answer with the distinction of in addition to one in the succession number to decide if the subsequent parcel relates to the first. blackhole/synergistic dark opening assaults in MANETs. In their proposed technique, every hub has its dubious worth, which depends on the unusual contrast saw between the steering messages communicated from the hub. Moreover, when the source hub gets the course answer (RREP) parcel in answer to the course demand (RREQ) bundle, they confirm the dubious worth of the hub that introduced the RREP bundle. As check, assuming this worth is higher than the edge level, the hub is considered as malignant and its location is put away in a boycott table, forestalling that hub to additionally partake in the steering interaction.

The proposed strategy in [12] projects a novel programmed security component utilizing Support Vector Machine (SVM) to protect against malignant assault happening measure. What's more, they have utilized the worth of bounce tally and the assessed time as contribution to these two calculations to choose the most limited secure way. An adjusted calculation to work on the security and execution of the AODV convention against the dark opening assault from in [14]. In this calculation, the creators utilized a few new principles to recognize the dangerous hubs as per the hub's practices in an Ad Hoc organize and erase them from directing. Our proposed strategy contrasts from the methods refered to on writing audit in that it centers around sending just the substantial course answer to the following hub, even on account of at least one blackhole assaults, by sending double a similar parcel answer with the distinction of in addition to one in the arrangement number to decide if the subsequent bundle compares to the first.

2.1. Security Requirements of VANET

A framework can be helpless against different framework shortcomings which can be abused by malevolent component for different reasons. To make a framework secure, the security prerequisites of a framework should be tended to. There are some security prerequisites of the VANET framework which are momentarily portrayed underneath. Likewise, figure 4 shows the sorts of potential assaults that can think twice about prerequisites in VANET [15].

Verification

One of the major and unquestionable prerequisites of any framework. A framework should know the genuineness of the relative multitude of members of the framework. Particularly, in VANET which is powerless against different adventures, the verification and distinguishing proof become vital and essential. On account of certain assaults in VANET, an incredible validation approach can give solid lawful verification against the gatecrasher. Subsequently, to shield the VANET framework from assaults, for example, Sybil assault, position assault, burrowing, replay assault, message adjustment and soon, the Authentication interaction is a conspicuous necessity.

Accessibility

A framework or a segment in a framework may confront disappointment or a few assaults. Such malevolent state of a part or a framework ought not influence different clients or components of the framework. In VANETs, every one of the applications and organizations ought to be

accessible and work in any event, when a component of VANET is enduring an onslaught. Some VANET hubs or foundation may confront a few assaults or issues which ought not influence different hubs. All in all, the assets of VANET should be consistently accessible. To accomplish the accessibility prerequisite in VANET, a powerful, secure and alter open minded framework configuration should be accomplished. There are different assaults like Denial of Services (DOS) assault, Black opening assault, spamming assault, Distributed Denial of Service (DDOS) assaults, and so on that can truly affect the accessibility necessity of VANET.

Classification

The messages traded between two parts in VANET ought not be presented to the third element. Classification can be accomplished by utilizing different encryption calculations. In VANET, the security messages don't have touchy information henceforth they are not scrambled. Nonetheless, the client related data like electronic installment, client's character, and other individual data are kept private with the assistance of different cryptographic calculations. Traffic investigation, Data mocking, and snooping are a portion of the likely assaults on privacy in VANET.

Respectability

Shields messages from manufacture or introduction. The messages sent and received by different substances of VANET ought to be kept flawless. Which implies the respectability of messages must be shielded from being altered by aggressors. The trustworthiness of messages can be affected by assaults, for example, Masquerade assault, Replay assault, Data change assaults, and so forth To safe guard messages during transmission and gathering, a protected convention should be carried out. In VANET, the IEEE1609.2 standard is utilized for security administrations.

Non-Repudiation

One of the significant security necessities of VANET. Non-Repudiation ensures a sender or a collector from forswearing of the communicated information from them [16]. VANET security prerequisites and the potential dangers to those necessities are laid out in figure 4below.

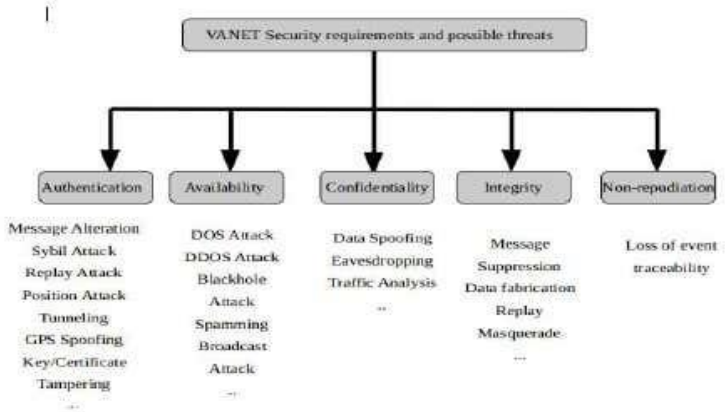


Figure 1

2.2. AODV Steering Convention

AODV is an improvement of the DSDV directing convention and quite possibly the most famous steering conventions in impromptu organizations. AODV convention uses DSDV's calculation by diminishing the transmissions and setting up courses just when requested or required. On account of such qualities of AODV, unnecessary memory and course repetition

are shortened and consequently it is reasonable for VANETs too. As in the majority of the receptive conventions, the information transmission happens in AODV just in an on-request state. AODV performs unicast just as multicast tasks. In General, AODV makes two strides for the activity which are as per the following:

3. SECURITY ISSUES IN VANET

Despite the fact that VANET innovation has improved and created lately, there are as yet numerous securities gives that exist in the framework. Little mistakes in a product application can cause genuine results in the VANET framework. The security part of VANET is an enormous test to get VANET from different assaults, protection issues, and data spillage. VANET actually has a lot of weakness which can be abused by the assailants. Before the appropriation of VANET in reality, the various layers of VANET should be made secure. Some different dangers and assaults are available in various layers of the VANET framework.

3.1. Blackhole Assaults

A dark opening assault is an assault against the trustworthiness of the organization in VANET. This sort of assault is dispatched in two stages. Initial, an assailant hub abuse conventions like AODV by promoting itself of having a superior course to the objective hub. The hub catches bundles and drops them in the subsequent advance. As the dark opening assault is the focal point of the theory, it is clarified exhaustively in a later part.

3.2. Countermeasures

The countermeasures of organization layer assaults generally rely upon the kind of directing convention utilized in VANET. By and large, different security instruments, for example, cryptography-based calculation, the trust-based methodology can be carried out to protect against assaults on the organization layer. Since this paper manages the dark opening assault on the AODV steering convention, a documented confirmation based methodology is received.

4. PROCLAMATION OF THE PROBLEM

Because of the idea of dynamic organization geography, steering in vehicular specially appointed organization play avital job in the exhibition of the organizations. Naturally, the majority of the security threats target directing conventions the most fragile place of the vehicular impromptu network. There are different examinations and exploration in this field trying to propose more secure protocols. Nonetheless, there is certifiably not a total directing convention that can altogether get the operation of one organization in each situation.

The bundles in the VANET contain profoundly significant and classified data and hence these parcels ought not be hampered or altered by malevolent parcels. In like manner, the drivers who update traffic data ought to likewise be exposed to responsibility by giving right and timely updates. Mobility, size of the organization and geographic significance makes it complex to implement security in VANET. By executing secure AODV steering conventions and running these directing conventions in malicious conditions, we trust that we will ensure the dark opening assault and further develop the performance of these safe directing conventions.

5. PROPOSED METHOD

As referenced previously, the majority of the steering conventions for Ad-hoc networks were created along time back without thinking about their security instrument. Consequently, those steering conventions are inclined to different assaults. In this segment, we will portray exhaustively our proposed answer for forestall the dark opening assault that we have

incorporated with the AODV directing convention. In our methodology like the standard AODV steering convention, the objective hub or halfway hub creates the RREP bundle however it additionally produces another RREP parcel.

It is a sort of affirmation of the primary parcel with a succession number augmented by one. Thusly, we have two RREP messages from the objective hub or a transitional hub that has the course to the objective one with the typical grouping number and the other with the ordinary succession number + 1 and both have the field VERIFIED set to 0. At the point when the halfway hub gets the RREP parcel it stores the data about the bundle answer then it checks our annexed field VERIFIED in case it is set to 0 or 1. In case it is 0 that implies that our parcel isn't yet confirmed or it is an invalid bundle in any case the parcel is checked and legitimate and it should be sent to the following hub.

0 1 2 3

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9+-+| **Type |R|A| Reserved | Verified | Prefix Sz | Hop Count** |+-+| **Destination IP address** |+-+| **Destination Sequence Number** |+-+| **Originator Sequence Number** |+-+| **Lifetime** |+-+

Figure 2 Format of the modified Route Reply (RREP) Message

In case of the field VERIFIED is 0 and the intermediate node receives a second route reply message it must verify if the first route reply's sequence number is the second reply's sequence number minus one; if the verification is true it sets the field VERIFIED to 1 and forward the packet.

Step 1: (Initialization process) Start the route discovery phase with the source node S.

Step 2: (Generation of RREPs)

The destination node or the intermediate node generates two route reply with two different destination sequence number, the second one must be incremented by one. Send Reply (seqno,

```
 // Dest Sequence Num VERIFIED = 0, );
// Appended field send Reply( seqno+1,
// Dest Sequence Num VERIFIED = 0, );
// Appended field
Step 3: (Verification of RREPs)
if ( intermediate node receives RREP )
{
if ( the first time the node receives RREP )
{
Store the IP address and seqno of the node;
if ( RREP is valid)
{
Forward RREP;
 }
}
 else if (the node receives more than one RREP )
{
```

```
Store the IP address and seqno of the node;
if ( RREP is invalid)
{
if ( new RREP's seqno == old RREP's seqno + 1)
{
VERIFIED = 1;
 //( Mark RREP as valid)Forward RREP;
}
 Else
 {
Ignore RREP;
 }
}
 else
{
Forward RREP;
 }
}
}
```

Step 4: (Continue default process)The source node sends data to the destination node from the selected route reply packet.

Also, when the intermediate node receives another route reply from the malicious node which performs a black hole attack with a very high destination sequence number. The same procedure explained will be repeated and in this case, the verification will be false, therefore, the intermediate node leaves the field VERIFIED set to 0 and ignores the packet. Our solution avoids the black hole attack and also a multiple black hole attack. In addition, the control messages from the malicious node, are not forwarded in the network.

6. METHODOLOGY F EVALUATION

6.1. Reenactment Environment

The reproductions are finished utilizing NS-2 (v-2.35) network test system [27] to investigate the exhibition of our proposed arrangement against dark opening hubs. In a space of 500x500 m, 25nodes are arbitrarily dispersed, they execute once the standard AODV and some other time the M-AODV (Modified AODV) directing convention for contrasting the two conventions under the blackhole assault. For the malevolent hubs are additionally haphazardly appropriated. Five sets were haphazardly picked for information correspondence, each sending 512 bytes each second. All hubs were moved in a Random-way point model, with irregular velocities going somewhere in the range of 0 and 30m/s. Likewise, the interruption season of the hubs is 10s. The reenactment boundaries are summed up in table 2.Therefore, every information point addresses a normal of twenty runs.

6.2. Measurements utilized for Simulation

To assess the exhibition of our methodology, we have utilized the accompanying measurements:

1) Packet Delivery Ratio (PDR)

It is the proportion of the all out various information bundles got by the objective hubs and the all out number of information parcels created by the source hubs. Thus, the parcel conveyance proportion shows the absolute number of information bundles that arrive at the objective effectively. A higher parcel conveyance proportion shows higher convention execution.

2) Average End-to-End Delay

It very well may be characterized as the time passed between the snapshot of sending of a piece by the source hub and the snapshot of its gathering by the objective hub. it incorporates all conceivable deferrals taken by the switch to look for the way in the organization, for example, buffering during course disclosure inactivity, lining at the interface line, engendering, retransmission delays at the MAC and move times. The normal start to finish delay is estimated in milliseconds.

3) Normalized Routing Overhead

This measurement means the quantity of steering control bundles created per information parcels communicated. It is called Normalized Routing Overhead or Normalized Routing Load.

Simulation Parameters

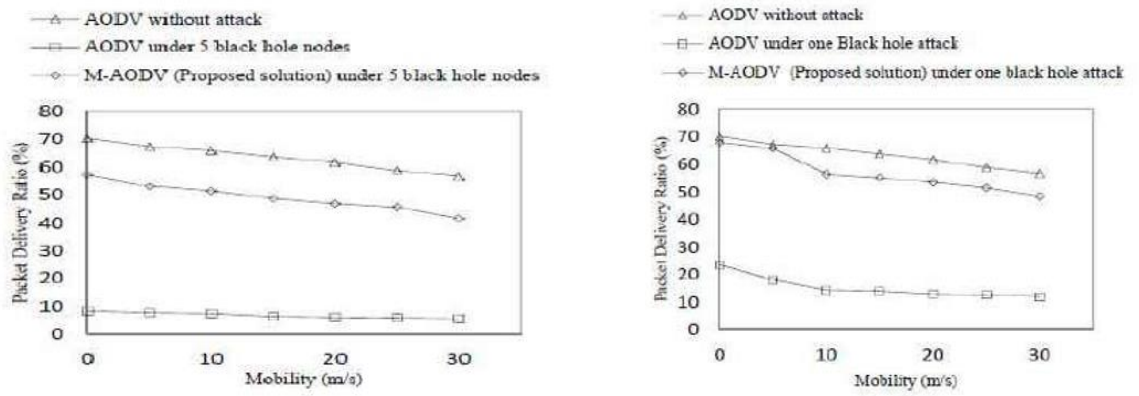
Parameter Value
Coverage Area 500x500 m
Number of nodes 25
Simulation time 200s
Transmission range 50m
Mobility model Random
Way point Data Rate 0.25
Packet Size 512 Bytes
Routing Protocol AODV / S-AODV
Mobility speed 0-30 m/s
No of black hole nodes 1 and 5
Connections 5
Traffic type UDP
–
CBRPause time 10s

7. SIMULATION RESULTS AND ANALYSIS

7.1. Packet Delivery Ratio

The Fig. 5 and the Fig. 6 show the packet delivery ratio of AODV, our solution and AODV under one black hole node and under-five black hole attackers when node mobility increases. It is clear from the figures that the performance of our approach is superior over AODV under a black hole attack either for one or multiple attackers. The PDR of AODV under one attack was approximately 15%, while the PDR of Modified AODV in the presence of one attack was approximately 60%, increased by 45%. Similarly, the PDR of AODV under multiple attacks was approximately 7%, which was increased by 43% when compared to our scheme also under multiple attacks. Moreover, the PDR of the AODV routing protocol without any attacks is

around 64%, which is due to congestion in the network.Fig.2 Packet delivery ratio vs. mobility with one attackerFig.3 Packet delivery ratio vs. mobility with five attackers



..

Figure 3

7.2. Normal End-to-End Delay

From the Fig. 7 and Fig. 8, it tends to be seen that, when the Modified AODV convention is utilized, there is an increment in the normal start to finish delay, contrasted with the norm. AODV directing convention without assault. Likewise, we see that our methodology under one assault is somewhat expanded in the normal start to finish delay, contrasted with under different assailants. This is because of the extra holding up time in each middle of the road hub prior to sending the answer, and when there is a various assault our methodology nee3d more opportunity to figure the right course answer than when one assault exists. The start to finish delay within the sight of aggressors in the AODV is the less in the two cases, either within the sight of one dark opening hub or within the sight of numerous assailants. This is a result of the prompt answer from the noxious hub, which doesn't check its steering table for the course accessibility.

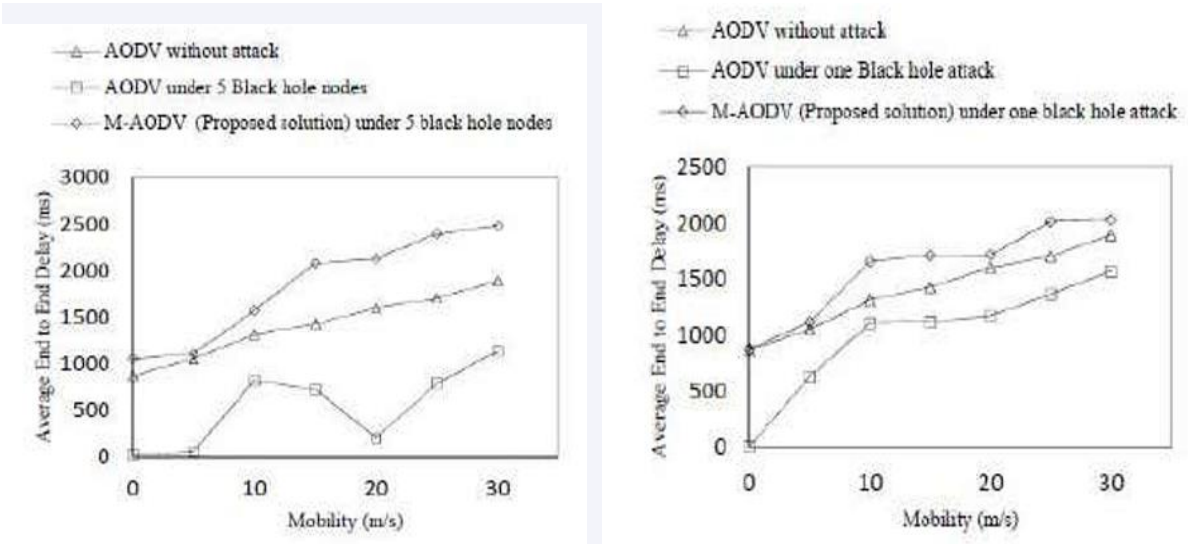


Figure 4

7.3. Standardized Routing Overhead

The standardized steering overhead is displayed in Fig. 6 and Fig. 7 while changing portability. In our adjusted AODV, the steering overhead under one or different malevolent hubs is somewhat higher contrasted with the standard AODV in light of the extra interaction required

to keep away from the determination of vindictive hubs. The standardized directing overhead for AODV under dark opening assault, regardless of whether one or various assaults is exceptionally high contrasted with the AODV without assault. This is because of the dark opening hubs that send bogus answers to the course demand bundles which compromise the directing convention then the convention begins acting mischievously and creating extra steering parcels.

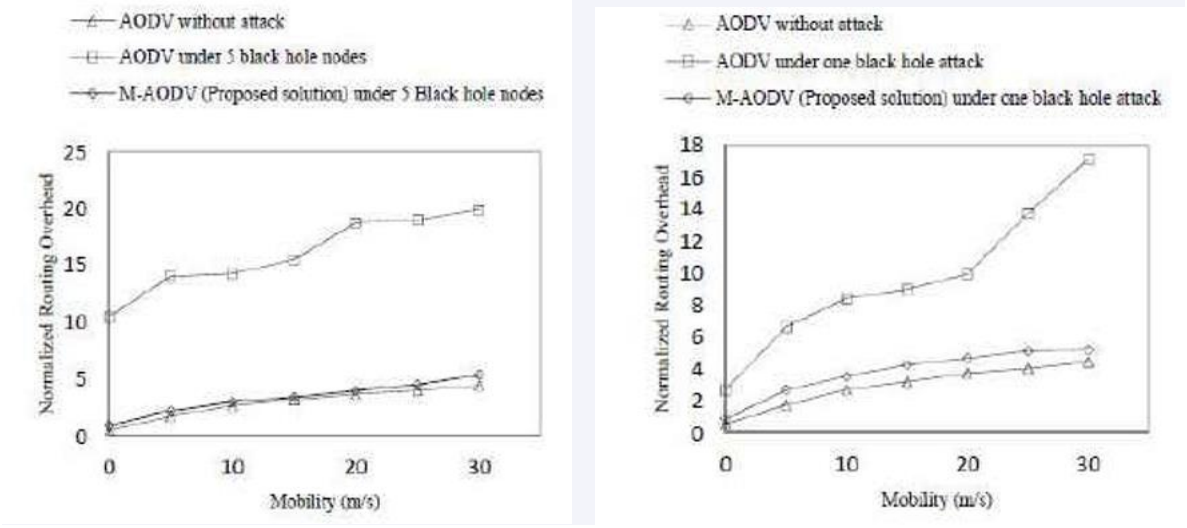


Figure 5

7.4. Assessment of the Number of the Dropped

Parcels by the Black Hole Attack in AODV and M-AODV We have determined the pace of the number of bundles sent, dropped and got in the two cases with one dark opening assault and five attackers in the standard AODV directing convention and furthermore in our changed AODV, as displayed in Fig. 8 and Fig. 9.In this reenactment, 25 hubs are moving haphazardly with greatest speed at 10 m/s, 10s for pause time, the quantity of associations is 5 and the quantity of bundles moving through the network is 2849 parcels. From the reproduction, we unquestionably affirm that our proposed scheme overcame the dark opening assault when there is a solitary dark opening assault and in any event, when there are numerous assailants. For the distinction between sent bundles and the amount of the parcels dropped and received packet is because of the parcels dropped if there should arise an occurrence of a crash or buffering or different reasons.

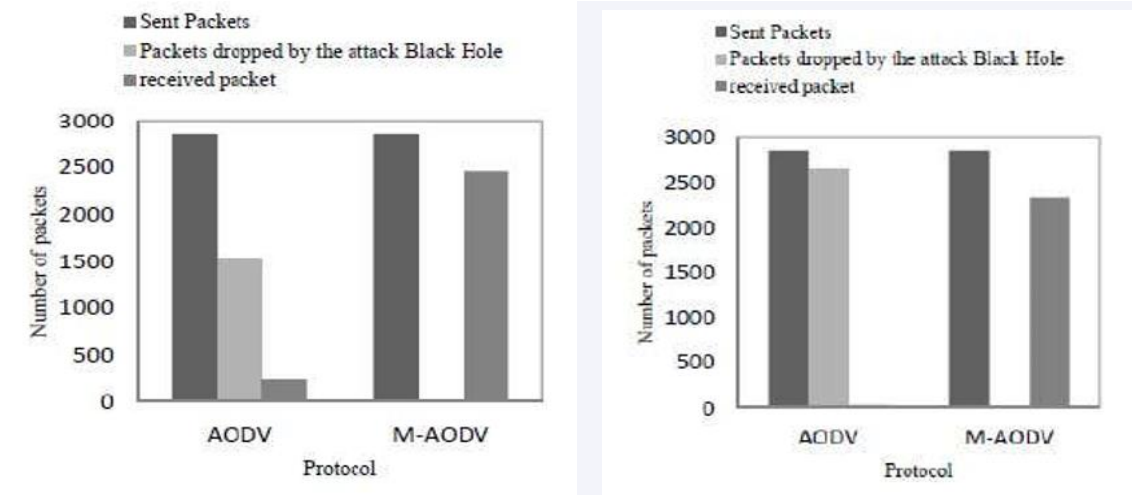


Figure 6

8. CONCLLUSION

Impromptu steering conventions are inclined to different assaults because of the obliviousness of the security angle during their plans. A dark opening assault upsets ordinary organization usefulness by sending false directing data during the course disclosure stage. In this paper, we proposed an answer for keep away from the dark opening and the various dark opening assailants on the AODV directing convention in VANETs. As indicated by the recreation results, the changed AODV gives a huge improvement in the bundle conveyance proportion with a satisfactory normal start to finish delay and standardized steering overhead when the versatility of hubs increments. Therefore, we inferred that our proposed approach shows unrivalled execution than the AODV within the sight of one or various dark opening hubs.

REFERENCES

[1] Salim Lachdhaf, Mohamed Mazouzi, and Mohamed Abid (2017), Detection and Prevention of Black Hole Attack in VANET Using Secured AODV Routing Protocol, International Conference on Networks& Communications, Dubai, pp. 25-36.

[2] HeithemNacer and Mohamed Mazouzi (2016), A Scheduling Algorithm for Beacon Message in Vehicular Ad Hoc Networks, International Conference on Hybrid Intelligent Systems, Marrakech, Morocco, pp. 489-497.

[3] R. GaneshBabu (2016), Helium's Orbit Internet Of Things (IOT) Space, International Journal of Computer Science & Wireless Security, Vol.03, No.02, pp.123-124.

[4] Elias C. Eze, Sijing Zhang and Enjie Liu (2014), Vehicular Ad Hoc Networks (VANETs): Current State, Challenges, Potentials and Way Forward, Proceedings of the 20th International Conference on Automation& Computing, Cranfield University, Bedfordshire, UK, p. 2014.

[5] S.Gurmukh, P.Kumari and S.Agrawal (2015), Comparative Analysis of Various Routing Protocols in VANET, In Proceedings of 5th IEEE International Conference on Advanced Computing & Communication Technologies, Haryana, India, p. 2015

[6] Sabihur Rehman, M. Arif Khan, Tanveer A. Zia, Lihong Zheng (2013), Vehicular Ad -Hoc Networks(VANETs) - An Overview and Challenges. Journal of Wireless Networking and Communications, pp. 29 -38.

[7] C. Perkins, Belding-Royer, E., & Das, S (2003), Ad hoc on-demand distance vector (AODV) routing, p. 356.

[8] Perkins, C. E. and Bagwig, P (1994), Highly dynamic destination-sequenced distance-vector routing(DSDV) for mobile computers, p. 1994.

[9] R.GaneshBabu, and Dr.V.Amudha (2015), Performance Analysis of Distributed coordinated Spectrum Sensing In Cognitive Radio Networks C, Middle East Journal of Scientific Research, Vol.23, No.23, pp.50-55.

[10] Johnson, D. B. and Maltz, D. A (1996), Dynamic source routing in ad-hoc wireless networks. In Mobile computing, Springer US pp. 153-181.

[11] P. Karthika and P.Vidhya Saraswathi (2017), Content Based Video Copy Detection Using frame Based Fusion Technique, Journal of Advanced Research in Dynamical and Control Systems, Vol. 9, No. 17, pp. 885-894.

[12] A.Nedumaran and V.Jeyalakshmi (2015), CAERP: A Congestion And Energy Aware Routing protocol For Mobile AD HOC Network, Indian Journal of Science and Technology. Vol.8, No.35, pp.1-6.

[13] Jaisankar, N., Saravanan, R. and Swaour, K. D (2010), A novel security approach for detecting black holeattack in MANET, In Information Processing and Management. Springer Berlin Heidelberg., p, pp. 217-223

[14] Patel, M. and Sharma, S (2013), Detection of malicious attack in manet a behavioral approach, In Advance Computing Conference (IACC), IEEE 3rd International, pp. 388-393.

[15] R.GaneshBabu, and Dr.V.Amudha (2016), Cluster Technique Based Channel Sensing Incognitive Radio Networks, International Journal of Control Theory and Applications. Vol.9, No.5, pp.207-213

[16] Wubishet Girma Mekonnen & Nedumaran Arappali Vol.3(Iss.2) 2020 (Jan)International Journal of Intelligent Computing and Technology (2457 0249) 15-16.

[17] Ghathwan, K. I. and Yaakub, A. R. B (2014), An Artificial Intelligence Technique for Prevent Black Hole Attacks in MANET, Recent Advances in Soft Computing and Data Mining. Springer International Publishing, (pp. 121-131)

[18] A.Nedumaran, S.AbdulKerim and Tedros Salih Abdu (2017), Advanced Link State Routing protocol Approach For Mobile Ad-Hoc Networks, International Journal for Scientific Research and Development. Vol. 5, No. 3, pp.516-519

[19] Shahabi, S., Ghazvini, M. and Bakhtiarian, M (2015), A modified algorithm to improve the security and performance of the AODV protocol against black hole attack, Wireless Networks, p. 2015

[20] Zhou, Y., Wu, D. and Nettles, S (2004), Analyzing and Preventing MAC-Layer Denial of Service Attack sfor Stock 802.11 Systems, p. 2004

[21] P.Karthika and P.Vidhya Saraswathi (2018), Digital Video Copy Detection Using steganography Frame Based Fusion Techniques, The International Conference on ISMAC in Computational Vision and Bio-Engineering, Lecture Notes in Computational Vision and Biomechanics, vol. 30. Springer, Cham

[22] Woungang, I., Dhurandher, S. K., Peddi, R. D. and Traore, I (2013), Mitigating collaborative black hole attacks on DSR-Based mobile ad hoc networks, In Foundations and Practice of Security, pp. 308-323

[23] Perkins, C., Belding-Royer, E. and Das, S (2003), Ad hoc On-Demand Distance Vector (AODV) Routing, p. 2003

[24] R.GaneshBabu and Dr.V.Amudha (2014), Spectrum Sensing Techniques In Cognitive radio NETWORKS: A SURVEY, International Journal of Scientific and Engineering Research. Vol.5, No.4, pp.23-32

[25] Network Simulator- NS-2 (2019), Available online: https://www.isi.edu/nsnam/ns/ (accessed on 5 May2019; no. May, p. 2019, 2019

[26] Yousefi, S., Mousavi, M. and Fathy, M (2006), Vehicular Ad hoc Networks (VANETs): challenges and perspectives, p. 2006

[27] Li, M. Security in VANETs. [online] Cse.wustl.edu.pdf

[28] Varshney, T (2019), Implementation of Watchdog Protocol with AODV in Mobile Ad Hoc Network, IEEE Conference Publication, p. 2019

[29] P.Karthika and P.Vidhya Saraswathi(2017), A Survey of Content Based Video Copy detection Using Big Data, International Journal of Scientific Research in Science and Technology, Vol. 3, No.5, pp. 114-118

[30] Thachil, F. and Shet, K (2019), A Trust-Based Approach for AODV Protocol to Mitigate Black Hole Attack in MANET, IEEE Conference Publication, p. 2019

[31] R.GaneshBabu, and Dr.V.Amudha (2015), Analysis Of Distributed Coordinated spectrum Sensing In Cognitive Radio Networks, International Journal of Applied Engineering Research. Vol.10, No.6, pp.5547-5552

[32] J. W. Cresswell (2002), Research Design: Qualitative, Quantitative and Mixed Methods Approaches, 2nd.Ed. California: Sage Publications, p.2002

[33] Rahul Krishnan, R.GaneshBabu, S.Kaviya, N.Pragadeesh Kumar, C.Rahul, and S.Santhana Raman (2017), Software Defined Radio (Sdr) Foundations, Technology Tradeoffs: A Survey, Proceedings of IEEE International Conference on Power, Control, Signals & Instrumentation Engineering (ICPCSI' 17) with ISBN.No-978-1-5386-0814-2, Saveetha Engineering College, Chennai, India, pp.2677-2682

[34] Nadeem, A. and Howarth, M. (2019), A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks. IEEE Journals & Magazine, p. 2019

[35] Tegegn Ayalew Hailu and A.Nedumaran (2019), A Survey On Provisioning Of Quality Of service (QOS) In MANET, International Journal of Research and Advanced Development, Vol. 3, No.2, pp.34-40

[36] Jalil, K., Ahmad, Z. and AbManan, J (2019), ERDA: Enhanced Route Discovery Mechanism for AODV Routing Protocol against Black Hole Attacks, p. 2019